MATH 347 HW9

Charles Swarts
swarts2@illinois.edu

November 2016

1 Q 1

1.1 a

Find the remainder of 1001^{1001} upon division by 9.

By the definition of modular congruence and $2.b$ (powers) from the last worksheet:

$$1001^{1001} \equiv (1001 - (111)9)^{1001} = 2^{1001} \bmod 9$$

Then using a combination of $2.a$ (multiplication) and $2.b$, we get the following progression

$$2^{1001} \equiv 2 \cdot 4^{500} \equiv 2 \cdot 16^{250} \equiv 2 \cdot 7^{250} \equiv 2 \cdot 49^{125} = 2 \cdot 4^{125} \equiv 2 \cdot 4 \cdot 16^{62} \equiv 8 \cdot 7^{62} \bmod 9$$

$$8 \cdot 7^{62} \equiv 8 \cdot 49^{31} \equiv 8 \cdot 4^{31} \equiv 8 \cdot 4 \cdot 16^{15} \equiv 32 \cdot 7^{15} \equiv 5 \cdot 7 \cdot 49^{7} \equiv 35 \cdot 4^{7} \equiv 8 \cdot 4 \cdot 16^{3} \bmod 9$$

$$\equiv 32 \cdot 7^{3} \equiv 5 \cdot 7 \cdot 49 \equiv 35 \cdot 4 \equiv 8 \cdot 4 \equiv 5 \bmod 9$$

So the remainder must be 5.

1.2 b

Using congruences show that 6 divides $n^3 + 5n$ for all $n \in \mathbb{N}$

To show that $6 \mid n^3 + 5n$, it is sufficient to show

$$n^3 + 5n \equiv 0 \bmod 6$$

By definition of congruence

$$n^3 + 5n \equiv n^3 + 5n - (n)6 \bmod 6$$

Using algebra we see

$$n^3 + 5n - 6n = n(n^2 - 1) = n(n+1)(n-2)$$

Note that it must be the case that n, or $n+1$, or $n+2$ is divisible by 3 because every third natural number is divisible by 3, and we go over 3 natural numbers. And it must be the case that n or $n+1$ is divisible by 2 by the same reasoning for 2.

Now to show the hypothesis is true, I have to lay down some theoretical frameworks. I did these for my benefit, feel free to skip them.

BEGIN FRAMEWORK

lemma: if $a, b \in \mathbb{N}$ are coprime, and if

$$\exists\, x, y \in \mathbb{Z} \text{ such that } xa \equiv ya \bmod b$$

Then

$$x \equiv y \bmod b$$

proof: suppose

$$xa \equiv ya \bmod b$$

Then by definition of congruence

$$\exists\, k \in \mathbb{N} \text{ such that } ax = ay + kb$$

Because a and b are coprime, they share no factors. By the fundamental theorem of arithmetic, the only way there is equality is if the prime factorization of the LHS matches the prime factorization of the RHS. Therefore it must be the case that a is a factor in k. So let $\alpha \in \mathbb{Z}$ such that $\alpha = k/a$. Then

$$x = y + \alpha b$$

And by the definition of congruence,

$$x \equiv y \bmod b$$

□

lemma: if $a, b \in \mathbb{N}$ are coprime, then there exist $d, e \in \mathbb{N}$ such that $da - eb = 1$

proof: since the hypothesis matches the definition of congruence it is sufficient to show

$$\exists\, d, \text{ such that } da \equiv 1 \bmod b$$

let $g, h \in [b]$ such that $g \neq h$

If $ga \equiv 1 \bmod b$ and $ha \equiv 1 \bmod b$ then

$$ga \equiv ha \bmod b$$

Because a and b are coprime, by the previous lemma

$$g \equiv h \bmod b$$

By definition of congruence for some $k \in \mathbb{Z}$

$$g = h + kb$$

Because $g, h \in [b]$, adding any non-zero lots of b to g excludes it from being in $[b]$. So $k = 0$. But then

$$g = h \;\; ※$$

So no two ga and ha have the same congruence mod b. So for all $d \in [b]$, each da is an element in a separate congruence class mod b.

Because there are only b congruence classes for mod b, and we have gone through b unique da values which each go into a separate congruence class mod$b$, there must be a value of d so that $ad \equiv 1 \bmod b$ □

lemma: if $a, b \in \mathbb{N}$ are coprime, then for $c \in \mathbb{N}$, if $a \mid c$ and $b \mid c$ then $a \cdot b \mid c$

Let $d, e \in \mathbb{N}$ such that

$$da - eb = 1$$

Which from the previous lemma we showed is always possible for these scenarios.

By definition of divides, if $a \mid c$ and $b \mid c$, then $\exists\, i, j \in \mathbb{Z}$ such that $ia = c$ and $jb = c$ Then

$$i(ab) = bc \qquad\qquad j(ab) = ac$$

$$(ei)(ab) = (eb)c \qquad\qquad (dj)(ab) = (da)c$$

$$(da)c - (eb)c = (dj)(ab) - (ei)(ab)$$

$$c(\cancelto{1}{(da) - (eb)}) = (ab)((dj) - (ei))$$

$$c = (ab)((dj) - (ei))$$

So by definition of divides, $ab \mid c$ □

END FRAMEWORK

Since 2 and 3 are coprime, by the last lemma since $2 \mid n(n+1)(n+2)$ and $3 \mid n(n+1)(n+2)$ then $2 \cdot 3 \mid n(n+1)(n+2)$ So

$$6 \mid n(n+1)(n+2)$$

By definition of divides and congruence, this is the same as saying

$$n(n+1)(n+2) \equiv 0 \bmod 6$$

And since we know

$$n^3 + 5n \equiv n(n+1)(n+2) \bmod 6$$

Then

$$n^3 + 5n \equiv 0 \bmod 6$$

Then by definition of congruence and divides

$$6 \mid n^3 + 5n$$

■

1.3 c

Using congruences, show that 7 divides $4^{3n+1} + 2^{3n+1} + 1$ for all $n \in \mathbb{N}$.

By definition of divides and congruence this is the same as asking to show

$$4^{3n+1} + 2^{3n+1} + 1 \equiv 0 \bmod 7$$

$$4 \cdot 64^n + 2 \cdot 8^n + 1 \equiv 0 \bmod 7$$

Let's focus on each term individually, by definition of congruence and using $2.a$ (multiplication) and $2.b$ (powers)

$$4 \cdot 64^n \equiv 4 \cdot (64 + (-9)7)^n \equiv 4 \cdot 1^n \equiv 4 \bmod 7$$

So the first term is always 7 mod congruent to 4.

$$2 \cdot 8^n \equiv 2 \cdot (8 + (-1)7)^n \equiv 2 \cdot 1^n \equiv 2 \bmod 7$$

So the second term is always 7mod congruent to 2.

$$1 \equiv 1 \bmod 7$$

Self explanatory

By the addition rule for congruence,

$$4 \cdot 64^n + 2 \cdot 8^n + 1 \equiv 4 + 2 + 1 \equiv 7 \equiv 7 + (-1)7 \equiv 0 \bmod 7 \ \checkmark$$

■

1.4 d

Using congruences, show that the number $13^{21} + 14^{14}$ is composite and find a nontrivial divisor of this number.

We know

$$13^{21} + 14^{14} = (13^3)^7 + (14^2)^7$$

Then build from the ground up

$$13^3 \equiv -14^2 \bmod (13^3 + 14^2)$$

By 2.b (powers),

$$\begin{aligned}(13^3)^7 &\equiv (-14^2)^7 \bmod (13^3 + 14^2)\\(13^3)^7 &\equiv -(14^2)^7 \bmod (13^3 + 14^2)\\(13^3)^7 + (14^2)^7 &\equiv 0 \bmod (13^3 + 14^2)\end{aligned}$$

By the definition of congruence

$$\exists\, k \in \mathbb{Z} \text{ such that } (13^3)^7 + (14^2)^7 = k(13^3 + 14^2)$$

By the definition of divides

$$(13^3 + 14^2) \mid (13^3)^7 + (14^2)^7$$

So (13^3+14^2) is a non-trivial divisor of $13^{21}+14^{14}$ and since it has a non-trivial divisor, it must also be composite ■

2 Q 2

Given $n \in \mathbb{N}$, let $t(n)$ denote the alternating sum of its decimal digits starting form the right. Prove that $n \equiv t(n) \bmod 11$.

Proof:

We know that

$$10 \equiv -1 \bmod 11$$

So for $n \in \mathbb{N}$

$$10^n \equiv (-1)^n \bmod 11$$

We know that numbers in base 10 are expressed as

$$\sum_{i=0}^{\infty} a_i \cdot 10^i$$

Where a is a sequence containing elements $0 - 9$.

By 2.1 (multiplication)

$$\sum_{i=0}^{\infty} a_i \cdot 10^i \equiv \sum_{i=0}^{\infty} a_i \cdot (-1)^i \bmod 11$$

The expression on the RHS is equivalent to $t(n)$. So n is equivalent to $t(n) \bmod 11$. ■

3 Q 3

Let $(347)_b = 3b^2 + 4b + 7$ be the base b number with digits 3,4,7.

3.1 a

Find, with proof, infinitely many bases b for which the number $(347)_b$ is divisible by 347.

The first lemma from the FRAMEWORK will be used.

Proof:

We start with the fact that

$$3 \cdot 10^2 + 4 \cdot 10 + 7 \equiv 0 \bmod 347$$

This is obvious because $3 \cdot 10^2 + 4 \cdot 10 + 7 = (1) \cdot 347$ so by definition of congruence, this must be true.

Now if we were to have a base, $b \in \mathbb{N}$ where $b \geq 8$ for which $347 \mid (347)_b$, then, by the definition of divides and congruence, it should be the case that

$$3 \cdot b^2 + 4 \cdot b + 7 \equiv 0 \bmod 347$$

We know that if

$$3 \cdot 10^2 \equiv 3 \cdot b^2 \bmod 347$$

$$10^2 \equiv b^2 \bmod 347$$

By imported lemma that since 347 is prime and thus coprime with 10 it is the case that

$$10 \equiv b \bmod 347$$

$$b \equiv 10 \bmod 347$$

And

$$4 \cdot 10 \equiv 4 \cdot b \bmod 347$$

$$10 \equiv b \bmod 347$$

$$b \equiv 10 \bmod 347$$

And

$$7 \equiv 7 \bmod 347$$

Then

$$3 \cdot b^2 + 4 \cdot b + 7 \equiv 3 \cdot 10^2 + 4 \cdot 10 + 7 \equiv 0 \bmod 347$$

So if

$$b \equiv 10 \bmod 347$$

This will be the case.

By definition of congruence,

$$\forall\, h \in \mathbb{Z} \qquad b = 10 + h \cdot 347$$

So for any base b such that $b > 8$ and $b = 10 + h \cdot 347$, it will be the case that $347 \mid (347)_b$. ■

3.2 b

Find, with proof, infinitely many bases b for which the number $(347)_b$ is divisible by 7.

Proof:

Using our knowledge about bases, and the definition of congruence and divides, we know this question is the same as wanting to find an infinite number of bases, $b \in \mathbb{N}$ where $b \geq 8$, such that

$$3 \cdot b^2 + 4 \cdot b + 7 \equiv 0 \bmod 7$$

An appropriate seed base would be the base with 7 in its prime factorization. The first number that satisfies this is 14.

$$3 \cdot (7 \cdot 2)^2 + 4 \cdot (7 \cdot 2) + 7 \equiv 0 \bmod 7$$

$$7\Big(3 \cdot 7(2)^2 + 4 \cdot 2 + 1\Big) \equiv 0 \bmod 7$$

By definition of congruence this is true if

$$\exists\, k \in \mathbb{Z} \qquad 7\Big(3 \cdot 7(2)^2 + 4 \cdot 2 + 1\Big) = 0 + (k)7 \qquad \checkmark$$

We know that if

$$4 \cdot b \equiv 4 \cdot 14 \bmod 7$$

$$b \equiv 14 \bmod 7$$

and

$$3 \cdot b^2 \equiv 3 \cdot (14)^2 \bmod 7$$

$$b^2 \equiv (14)^2 \bmod 7$$

Which would follow if

$$b \equiv 14 \bmod 7$$

and

$$7 \equiv 7 \bmod 7$$

Then

$$3 \cdot b^2 + 4 \cdot b + 7 \equiv 3 \cdot 14^2 + 4 \cdot 14 + 7 \equiv 0 \bmod 7$$

So if

$$b \equiv 14 \bmod 7$$

This will be the case

By definition of congruence,

$$\forall\, h \in \mathbb{Z} \qquad b = 14 + 7h$$

So for any base b such that $b > 8$ and $b = 14 + h \cdot 7$, it will be the case that $7 \mid (347)_b$. ■

4 Q 4

4.1 a

$S = \mathbb{N}. x \sim y \Leftrightarrow x \mid y$

Proof of reflexive property.

By definition $x \mid x$ is true if

$$\exists\, z \in \mathbb{Z} \text{ such that } x = z \cdot x$$

if $z = 1$ then this becomes

$$x = (1)x$$

This is true for natural numbers.

So $x \sim x$ is true. By definition of reflexive, so is $\sim$. □

Counter-example to disprove symmetric property

1 divides 2, but 2 doesn't divide 1. So $x \sim y \not\Rightarrow y \sim x$. So $\sim$ isn't symmetric.

Proof of transitive property

if $x \sim y$ and $y \sim z$, then $x \sim z$, then it is transitive.

So $x \mid y$ and $y \mid z$. By definition of divides

$$\exists\, k, l \in \mathbb{Z} \text{ such that } y = kx \quad z = ly$$

$$z = (lk)x$$

Since an integer times an integer is an integer, (lk) is an integer.

By definition of divides,

$$x \mid z$$

So $x \sim z$. Therefore the hypothesis implied the conclusion and the relation is transitive. □

So this is not an equivalence relation because it isn't symmetric.

4.2 b

$$S = \mathbb{R}. x \sim y \Leftrightarrow \mid x - y \mid \leq 1$$

Proof of reflexivity:

If $x \sim x$ then the relation if reflexive.

If $\mid x - x \mid \leq 1$ is true then the relation if reflexive.

$$\mid x - x \mid = \mid 0 \mid = 0$$
$$0 \leq 1 \qquad \checkmark$$

So the relation is reflexive. □

Proof of symmetry:

If $x \sim y$ implies $y \sim x$, then the relation is symmetric.

If $| x - y | \leq 1$ implies $| y - x | \leq 1$, then the relation is symmetric.

$| x - y | \leq 1$ is the same as saying

$$-1 \leq x - y \leq 1$$

Multiplying all sides by -1 yields

$$1 \geq y - x \geq -1$$

Which is the same as saying

$$| y - x | \leq 1$$

So $| x - y | \leq 1$ implied $| y - x | \leq 1$, and the relation is symmetric. □

Counter-example for transitivity:

$| 2 - 1 | \leq 1$ and $| 1 - 0 | \leq 1$ but $| 2 - 0 | \nleq 1$

So this is not an equivalence relation because it isn't transitive.

5 c

$$S = \mathbb{R}. x \sim y \Leftrightarrow x - y \in \mathbb{Z}$$

Proof of reflexivity:

If $x \sim x$, then $\sim$ is reflexive.

If $x - x \in \mathbb{Z}$, then $\sim$ is reflexive.

$$x - x = 0$$

$$0 \in \mathbb{Z}$$

So $x \sim x$ and the relation is reflexive. □

Proof of symmetry

If $x \sim y$ implies $y \sim x$, then the relation is symmetric.

If $x - y \in \mathbb{Z}$ implies $y - x \in \mathbb{Z}$, then the relation is symmetric.

If $x - y \in \mathbb{Z}$, then $\exists\, k \in \mathbb{Z}$ such that $x - y = k$.

$$-k = y - x$$

Since multiplying an integer by -1 creates an integer, $-k \in \mathbb{Z}$

So $y - x \in \mathbb{Z}$.

So $x \sim y$ implied $y \sim x$ and the relation is symmetric. □

Proof of transitivity:

If $x \sim y$ and $y \sim z$ imply $x \sim z$, then the relation is transitive.

If $x - y \in \mathbb{Z}$ and $y - z \in \mathbb{Z}$ imply $x - z \in \mathbb{Z}$, then the relation is transitive.

If $x - y \in \mathbb{Z}$ and $y - z \in \mathbb{Z}$, then $\exists\, k, l \in \mathbb{Z}$ such that $x - y = k$ and $y - z = l$.

$$x - y + y - z = k + l$$

$$x - z = k + l$$

Since an integer plus an integer is an integer, $k + l$ is an integer.

So $x - z \in \mathbb{Z}$.

Since $x - y \in \mathbb{Z}$ and $y - z \in \mathbb{Z}$ implied $x - z \in \mathbb{Z}$, the relation is transitive. □

So the relation is an equivalence relation because it is reflexive symmetric and transitive.

5.1 d

$$S = \mathbb{R}. x \sim y \Leftrightarrow \text{ “There exists” } n \in \mathbb{Z} \text{ such that } x = 2^n y$$

We can rearrange this a little to be if

$$\text{“There exists” } n \in \mathbb{Z} \text{ such that } x - 2^n y = 0$$

Since $x, 2^n y \in \mathbb{R}$ and $0 \in \mathbb{Z}$, if there does exist n, then the problem takes on the general form of problem (c).

So I would say this relation is reflexive symmetric, and transitive, and also an equivalence relation.